Listing of Claims

1. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably disposed thereon ~~residing therewith~~ for enabling said first SSL connection between said client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing with~~ said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

2. (Previously presented) The system of claim 1, wherein said SSL acceleration client

software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection.

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Cancelled).

8. (Cancelled).

9. (Previously presented) The system of claim 1, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

10. (Cancelled).

11. (Currently amended) A method for increasing data access in a secure socket layer network environment, which includes the steps of:

employing a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and employing a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably disposed thereon ~~residing therewith~~ for enabling said first SSL connection between said client and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing with~~ said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software through SSL acceleration server software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

12. (Previously presented) The method of claim 11, wherein said SSL acceleration monitors when said web browser requests said first SSL connection with said web server computer and intercepts said SSL request from said web browser, and diverts communication through said second SSL connection.

13. (Cancelled).

14. (Cancelled).

15. (Cancelled).

16. (Cancelled).

17. (Cancelled).

18. (Cancelled).

19. (Previously presented) The method of claim 11, which includes employing compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

20. (Cancelled).

21. (Cancelled).

22. (Cancelled).

23. (Cancelled).

24. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a second computer communicatively linked to said web server computer operably associated with web browser software having SSL protocol client software operably disposed thereon ~~residing therewith~~ for enabling said first SSL connection between a client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing~~ said second computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to said SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

25. (Previously presented) The system of claim 24, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection.

26. (Previously presented) The system of claim 24, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.